CB PROTECTION

Operating Environment Requirements (OER)

Version 8.1.8, April 2020

Contents

Overview 2
CB Protection Server Requirements 2
CB Protection Server: Supported Operating Systems 2
CB Protection Database: Supported SQL Server Versions 2
CB Protection Database: Supported AWS RDS MS SQL Server Versions 2
CB Protection Web Server Platform: Support Server 3
CB Protection Console: Supported Browsers 4
CB Protection Server System Requirements 4
CB Protection Server Architecture by Endpoint Count 5
Notes on SQL Server Edition 5
Two-tier Deployment Architecture 6
CB Protection Database: SQL Storage Requirements 7
Special considerations for PCIe (PCI-express) flash storage: 7
CB Protection Database: SQL Memory Configuration 8
CB Protection Database: SQL Maintenance 8
CB Protection Database: SQL Backups 8
CB Protection Server: Virtualization 8
CB Protection Server: Common Performance Pitfalls 9
CB Protection Server: Communication Requirements 9
CB Protection Agent Requirements 10
CB Protection Agent Supported Operating Systems: 10
CB Protection Agent: Hardware Recommendations 10
CB Protection Agent Communication Ports 11
CB Protection Agent: Certificates 11

VMware, Inc. | 1100 Winter Street, Waltham, MA 02451 USA | Tel: 617.393.7400

Overview

This document describes the hardware, software and site requirements for implementing a CB Protection Server installation. *It is a requirements summary only*. For a successful server installation, you must use the *Installing CB Protection Server* manual for detailed descriptions of installation procedures. For successful agent installations, you must use the instructions in the "Managing Computers" chapter of *Using CB Protection*. If there are any questions related to hardware and performance, please contact your Carbon Black technical representative after reviewing this document.

CB Protection Server Requirements

CB Protection Server: Supported Operating Systems

Operating System	Architecture	Service Pack	Additional Notes/Requirements
Windows Server 2008 R2	x64	SP1 Or Later	HVM Virtualization only
Windows Server 2012 R2	x64	Use Latest	HVM Virtualization only
Windows Server 2016	x64	Use Latest	HVM Virtualization only
Windows Server 2019	x64	Use Latest	HVM Virtualization only

CB Protection Database: Supported SQL Server Versions

Database System	Architecture	Service Pack	Additional Notes/Requirements
SQL Server Express 2008 R2	x64	Use Latest	Limited to 1 CPU Socket (or 4 cores) Maximum memory utilized: 1Gb Maximum database size: 10Gb
SQL Server 2008 R2	x64	Use Latest	
SQL Server Express 2012	x64	Use Latest	Limited to 1 CPU Socket (or 4 cores) Maximum memory utilized: 1Gb Maximum database size: 10Gb
SQL Server 2012	x64	Use Latest	Standard edition for < 30K endpoints, Enterprise edition for larger deployments. See "CB Protection Server Architecture by Endpoint Count" below for more details.
SQL Server 2014	x64	Use Latest	Same as SQL Server 2012.
SQL Server 2016	X64	Use Latest	Same as SQL Server 2012
SQL Server 2017	X64	Use Latest	Same as SQL Server 2012

CB Protection Database: AWS RDS MS SQL Server Usage

Database System	Architecture	Additional Notes/Requirements
SQL Server Express	x64	Limited to 1 CPU Socket (or 4 cores) Maximum memory utilized: 1Gb Maximum database size: 10Gb
SQL Server Standard	x64	Standard edition for < 10K endpoints, Enterprise edition for larger deployments. See "CB Protection Server Architecture by Endpoint Count" below for more details.
SQL Server Enterprise	x64	Standard edition for < 10K endpoints, Enterprise edition for larger deployments. See "CB Protection Server Architecture by Endpoint Count" below for more details.

CB Protection Web Server Platform: Support Server

Common Requirements ①	Restrictions ②
In the IIS Roles Manager, verify the following configuration: • Common HTTP Features: - Static Content - Default Document - HTTP Errors - HTTP Redirection • Application development: - ASP.NET (version 4.5) - .NET Extensibility (version 4.5) - CGI - ISAPI Extensions - ISAPI Filters • Health & Diagnostics: - HTTP Logging - Logging Tools - Request Monitor - Tracing • Security: - URL Authorization - Request Filtering - IP and Domain Restrictions • Performance: None • Management Tools: - IIS Management Console - IIS Management Scripts and Tools - Management Service • FTP Publishing Service: None	Beginning with v8.0.0, the console relies on the CB Protection API. An incorrectly configured IIS server can prevent console access. • To confirm API functionality, go to **System Configuration > Advanced Options** in your current console and check the "API Access Enabled" box. If a green dot appears next to the checkbox, then you can assume that IIS is configured correctly. Otherwise, make sure you meet the following restrictions: • Site Bindings: The CB Protection API will not connect to localhost if the console web application is bound to a specific IP address instead of '*'. Make sure that '*' is added to the list of bindings. • IP Address and Domain Restrictions: If you must limit console access to specific IP addresses, be sure that the IPv6 localhost address is added to the list. • Application Pools: CB Protection must be run within the DefaultAppPool application pool. Using a different app pool results in the CB Protection server not having the appropriate credentials to access the SQL Server database. • Authentication: You must disable Basic Authentication and Windows Authentication so that the CB Protection Server handles authentication. Otherwise, users will not be able to log into the CB Protection Server.

Version	Part Of OS	Supported Architecture	Supported Level	Additional Notes/Requirements
IIS 8.5	Windows 2012 Server R2 only	x64		① ② Common Requirements and Restrictions are listed in the table above Additional requirements: Private memory for IIS should be increased to 800 MB
IIS 10	Windows 2016 Server / Windows 2019 Server	X64		① ② Common Requirements and Restrictions are listed in the table above Additional requirements: Private memory for IIS should be increased to 800 MB

CB Protection Console: Supported Browsers

Browser	Version	Additional Notes/Requirements
Microsoft Internet Explorer	11	Windows only
Mozilla Firefox	Latest	Windows, Mac or Linux
Google Chrome	Latest	Windows, Mac or Linux
Safari	13	Mac

CB Protection Server System Requirements

- Clean operating system installation, with the latest version/patch/service pack
- Microsoft IIS: Version corresponding to the Windows Server installed. Configured as described in the Installing CB Protection Server guide
- Microsoft .Net: Version 4.5.2 or later framework with latest patch level
- Microsoft Installer: Version 4.5 or newer
- Processor: Intel Xeon/i7 processor/multi-core running at least 2.5GHz. Although Intel processor is recommended, it is possible to use equivalent AMD processor
- Ethernet connection: 1 Gbps or faster connection required

CB Protection Server Architecture by Endpoint Count

The CB Protection Server should be deployed on a single computer that will house both the CB Protection Server and SQL Server. The following table lists the requirements for this computer.

Endpoints	SQL Server Edition	Hardware		Required Database Storage		DAS (Locally attached)		PCIe Flash GB / 1K EPTS[2]
		RAM (GB)	CPU Cores[1]	SQL 2016 and Earlier	SQL 2016 SP1 and Later[4]	Disks	RAID	
Up to 100	Express	4	2	20 GB[3]	20 GB[3]	2	1	n/a
101 – 250	Standard	12	2	55 GB	50 GB	4	1+0	n/a
251 - 500		16	2	100 GB	90 GB	4	1+0	n/a
501 – 1,000		16	4	175 GB	150 GB	6	1+0	n/a
1,001 – 1,500		16	4	300 GB	260 GB	6	1+0	n/a
1,501 – 2,000		16	4	500 GB	440 GB	8	1+0	n/a
2,001 – 5,000		32	6	1 TB	900 GB	8	1+0	n/a
5,001 - 10,000		48	8	1.2 TB	1 TB	12	1+0	n/a
10,001 – 20,000		48	8	2 TB	1.75 TB	14	1+0	50
20,001 – 30,000		128	16	3 TB	2.5 TB	24	1+0	50
10,001 - 40,000	Enterprise	64	12	2 TB	2 TB	12	1+0	20
40,001 - 80,000		96	16	4 TB	4 TB	14	1+0	20
80,001 - 160,000		96	16	8 TB	8 TB	22	1+0	20

[1] *CPU core requirements are based on physical, not hyper-threaded cores. Two CPUs might be necessary to reach required number of cores.*
[2] *PCIe sizing requirement is given in GB per 1K endpoints.*
[3] *Database storage for SQL Express includes 10 GB for data file (maximum limit for SQL Express) and additional 10 GB for the log file.*
[4] *Index compression will only be enabled for new installs. Upgrades should reference the SQL 2016 and Earlier column.*

Associated with the storage sizes listed above are the following caveats:

- By default, the CB Protection Server saves no more than four weeks of events and no more than ten million events. Increasing these defaults will increase the size of the database. Under normal circumstances, the largest portion of the database will be taken up with storage of instances of files on endpoints.
- The CB Protection Server carries out two scheduled database tasks described in the document *SQL Server Configuration for CB Protection*. Stopping these tasks can cause the database to grow beyond the sizes listed above.
- The steps listed under “Database Growth” in the document *SQL Server Configuration for CB Protection* are being followed.

Notes on SQL Server Edition

Deployments with 10,000 to 30,000 endpoints have a choice of SQL Server editions. When using SQL Server Standard, keep the following points in mind:

- With over 20,000 endpoints, SQL Server 2014, 2016, or 2017 must be used. Earlier versions of SQL Server Standard do not support enough RAM or CPU Cores.
- Unlike SQL Server Enterprise, SQL Server Standard prior to SQL Server 2016 SP1 does not use data compression. This is why it needs more memory and disk space.

- On SQL Server Standard, CB Protection achieves equivalent performance processing file inventory compared to SQL Server Enterprise, but the CB Protection console can be 30% slower and some database maintenance tasks such as rebuilding indexes and statistics will be slower. This can be mitigated by placing the database on faster storage hardware.

Two-tier Deployment Architecture

Here are the requirements for a two-tier installation of the CB Protection where the CB Protection Server and SQL Server reside on separate hardware:

1. For the SQL Server hardware, use the single-tier table above.
2. For the CB Protection Server hardware, use the following table:

Endpoints	Hardware	
	RAM (GB)	CPU Cores[1]
Up to 1,000	4	2
1,001 - 80,000	8	4
Above 80,000	16	8

[1] *CPU core requirements are based on physical, not hyper-threaded cores. Two CPUs might be necessary to reach required number of cores*.

3. Make sure that the network latency between the CB Protection Server and SQL Server is 0.7 ms or lower. The freeware utility hrPing or similar can be used to validate the latency.
4. The SQL server instance and underlying database storage has to be dedicated to the CB Protection Server

CB Protection Database: SQL Storage Requirements

The SQL database should meet the following requirements:

- The OS and paging file must be on a separate physical partition from the SQL database. Use of two additional disk drives configured as a RAID-1 partition (mirror) is recommended.
- Any AV software must be configured to exclude SQL data directories.
- Direct attached storage (DAS) is required, using a 6 GB/s SAS (Serial Attached SCSI) adapter or better.
- All hard drives must be 2.5" in size, and have rotational speed of 15K RPM. Note that for deployments larger than 40,000 endpoints, 10K RPM drives can be used if the total required disk size requirement cannot be met with available 15K RPM drives.
- RAID-10 should be used with DAS drives
    - Stripe element size: 64 KB
    - Controller cache-write policy: “Write Back”
- Performance of SQL storage should be validated with the Bit9SQLIO tool prior to deployment of CB Protection Server.
- When PCIe Flash storage is not used, the entire database (data + log + indexes + temp) should be on the single large DAS partition. Total disk space shown in the table above includes both hard drive and flash drive space.
- The table shows that Enterprise SQL server requires less storage per endpoint. The reason is that this edition of SQL server supports compression, which reduces storage requirements for more than 50%.

Special considerations for PCIe (PCI-express) flash storage:

- Use of a PCIe card is required when noted in the sizing table.
- Carbon Black recommends a NVMe x8 MU Card[1] from any major vendor.
- When PCIe Flash storage is used, you should partition the database so that indexes go to the flash storage partition and all other files (data + log + temp) go to the single large DAS partition. Check table above for PCIe card space requirements per 1K endpoints.
- Even though it is not required, in order to further improve product performance, the entire database except for the log file (data + indexes + temp) can be moved to flash storage. Security teams who require extremely fast search response times may opt for such an option. This will require 100 GB of flash storage for every 1K endpoints for SQL Standard edition, or 50GB per 1K endpoints for SQL Enterprise edition.
- When PCIe flash storage is used, card airflow requirements have to be met by the hardware box.
- Transaction logs should remain on SAS disks or other storage optimized for sequential writes.

[1] 1 NVMe = non-volatile memory express
X8 = motherboard PCIe 3.0 or 4.0 - x8 interface
MU = mixed use
Card = usually a half height form factor (looks like a graphics card)

CB Protection Database: SQL Memory Configuration

Since the CB Protection Server database is relatively large, SQL Server will take all the RAM it has at its disposal, potentially leading to system memory starvation. For that reason, a SQL Server memory cap should always be set on SQL Server. On systems with 16GB RAM, set the memory cap to 12GB. For systems with more RAM, make sure that the SQL maximum server memory is set to at least 5 GB less than the total RAM installed in the system for SQL Server Standard, and 10 GB for SQL Server Enterprise edition.

Note: In a small configuration with SQL Server Express, there is no need to set a SQL memory cap because SQL Server Express already limits memory use to 1 GB.

CB Protection Database: SQL Maintenance

CB Protection Server does its own scheduled SQL DB Maintenance tasks on daily and weekly basis. This functionality is important in order to maintain database performance and limit growth. The maintenance tasks include:

- Deleting obsolete data
- Defragmenting indexes
- Rebuilding statistics

Note: Use of any other, custom maintenance tasks would be counter-productive and should be avoided.

CB Protection Database: SQL Backups

The CB Protection database uses the “Simple” recovery model. The “Full” recovery model should not be used to avoid a performance penalty and excessive database log growth.

CB Protection Server supports automated database backups, but only for deployments up to 100 endpoints. In all other cases, full database backups should be done using best SQL server practices. Also, a database consistency check should be done prior to backup to ensure that the database is not corrupt.

Recommended backup frequency is 2-3 full backups per week. More frequent backups might negatively impact server performance.

Database backup can run anywhere from minutes to hours, depending on database size, network speed (when backups are sent over the network) and performance backup storage. Backups impact server performance should be avoided during busy times (e.g. when many users rely on console performance), or during internal CB Protection Server maintenance times (see table below).

Maintenance Task	Times
Daily Cleanup Task	Every day at 12 AM (midnight), CB Protection Server local time. Task can run anywhere from 1 to 4 hours.
Database Index Maintenance	Every Saturday starting at 4 AM. Task can run anywhere from 2 to 6 hours.

CB Protection Server: Virtualization

CB Protection supports the use of virtualized environments for its deployment if the environment is smaller than 5,000 endpoints. Virtual environments must meet the minimum hardware configurations listed in the tables above, and also must meet the following requirements:

- VMware ESX Server 5.5U2+; recommend patching to current level

- SQL and CB Protection Server must be installed on the same virtual machine
- Memory must be allocated as “reserved”
- For virtualized servers, the underlying disk architecture must still meet aforementioned minimum requirements. *Physical DAS storage*, solely dedicated to the CB Protection VM, is preferred, but SAN storage may be used instead, if it meets these criteria:
    - IO channel: Fibre channel
    - Sequential write latency: 0.85ms or faster
        - Measured as 40kb writes, one thread, over two hours
    - Random write latency: 1.75ms or faster
        - Measured as 8kb writes, 32 threads, over two hours

  15K SAS drives for SQL logs and SSD drives for the other SQL storage should meet these criteria.

CB Protection Server: Common Performance Pitfalls

There are several pitfalls when purchasing and configuring hardware for the CB Protection Server. This section lists most common mistakes.

Category	Problem Explanation	Possible Mitigations
Slow SQL Storage	Misconfigured or slow storage used for SQL database files can significantly impact the ability of the server to process agent events and file changes and can cause a backlog of server tasks and slow console response.	1. Use direct-attached storage with correctly sized disks and RAID architecture 2. Avoid using SAN storage due to high latency 3. For larger deployments, use fast SSD/Flash storage, as documented
Slow Network	A slow network connection between the CB Protection Server and SQL Server can significantly impact the ability of the server to process agent events and files. This can cause a backlog of messages and loss of visibility into the agent inventory and operation.	1. Deploy CB Protection in a 1-tier model, with both the CB Protection server and SQL Server on the single machine 2. Reduce network latency between CB Protection and SQL server by using fewer, faster switches, or a direct cable connection
Resource Sharing	Shared SQL server or SQL storage layer can impact overall server performance because the server cannot utilize hardware resources as needed. Also, sharing introduces a varying load which makes it impossible to predict future server performance.	1. Provide a dedicated SQL server instance to the CB Protection 2. Provide dedicated storage to CB Protection SQL storage files, not used by either other databases or other applications
Hardware Virtualization	Improperly virtualized server hardware or virtualizing the server for a large number of endpoints can impact the overall server performance. The impact can be on either the network, CPU, memory or storage layer. As a reminder, virtualization is supported only below 5,000 endpoints.	1. Move product to physical hardware 2. Move product to 1-tier virtual hardware 3. Ensure that the virtual machine satisfies OER requirements (CPU, Memory), uses physical storage, and that there is very low latency between the CB Protection and SQL servers in case of 2-tier deployment

CB Protection Server: Communication Requirements

Requirement	Details	Additional Notes
Port 443 access	Outbound SSL From CB Protection Server to CB Protection Knowledge	Allow connection to services.bit9.com (proxy connections are supported)

Requirement	Details	Additional Notes
	Inbound HTTPS from CB Protection Console users and CB Protection Agents (for software upgrades)	
Inbound Port 41002 access	Inbound SSL from CB Protection agents	Port is configurable
Outbound Port 514 access	Outbound UDP for Syslog/SIEM connections	Optional, if Syslog/SIEM integrations are enabled. Port is configurable
Ethernet connection	1 GB/s connection required for connection to CB Protection Agents	
Static IP address only	(no DHCP) with an assigned FQDN or alias; IPv4 and/or IPv6 supported	
AD Integration	Server must be a member of a domain if AD integration is utilized	
Bandwidth	For every 1000 agents, you can expect server bandwidth to average about: • Inbound: 200kb/s • Outbound: 50kb/s	

CB Protection Agent Requirements

CB Protection Agent Supported Operating Systems:

Please refer to the "Supported Carbon Black sensors and agents" document on the Carbon Black User eXchange: https://community.carbonblack.com/docs/DOC-7991.

CB Protection Agent: Hardware Recommendations

Agent systems should be in compliance with all hardware requirements for the OS you are running. Consider all processes that run on the agent systems when determining hardware configuration.

It is important to note that only industry standard desktop, laptop or notebook computers as well as server hardware platforms are supported. Mobile, tablet, embedded or fixed-function devices require additional qualifications. Please contact Carbon Black Support for additional information.

Requirement	Details	Additional Notes
Memory	The Agent typically uses 50-100MB of virtual memory	
	Systems running WePOS, POSReady, XP Embedded or Embedded 7 should have at least 512MB of physical memory	
	Other supported operating systems should have at least 1GB of physical memory	
Disk Space	The Agent requires at least 200MB of free disk space on the system volume; 500MB is recommended.	Actual storage requirements depend on factors such as the number of files on the computer and the CB Protection Server configuration.
	If CB Protection is installed to a location other than the system volume, 100MB of free space must be available on the installation volume.	

CB Protection Agent Communication Ports

Requirement	Details	Additional Notes
Port 41002	From CB Protection Agent inbound to CB Protection Server on TCP port 41002 (configurable)	
Port 443	From CB Protection Agent inbound to CB Protection Server on TCP port 443 for CB Protection Agent upgrade	(Optional) Can be configured to use a Windows file server instead

CB Protection Agent: Certificates

Make sure your root certificates are up to date and not expired. Additionally, it is important to have your CRL (Certificate Revocation List) up to date.